POLYNOMIAL CUNNINGHAM CHAINS

LENNY JONES

ABSTRACT. Let $\epsilon \in \{-1, 1\}$. A sequence of prime numbers $p_1, p_2, p_3, \ldots$, such that $p_i = 2p_{i-1} + \epsilon$ for all i, is called a *Cunningham chain* of the first or second kind, depending on whether $\epsilon = 1$ or -1 respectively. If k is the smallest positive integer such that $2p_k + \epsilon$ is composite, then we say the chain has length k. Although such chains are necessarily finite, it is conjectured that for every positive integer k, there are infinitely many Cunningham chains of length k. A sequence of polynomials $f_1(x), f_2(x), \ldots$, such that $f_i(x) \in \mathbb{Z}[x]$, $f_1(x)$ has positive leading coefficient, $f_i(x)$ is irreducible in $\mathbb{Q}[x]$, and $f_i(x) = xf_{i-1}(x) + \epsilon$ for all i, is defined to be a *polynomial Cunningham chain* of the first or second kind, depending on whether $\epsilon = 1$ or -1 respectively. If k is the least positive integer such that $f_{k+1}(x)$ is reducible over $\mathbb{Q}$, then we say the chain has length k. In this article, for chains of each kind, we explicitly give infinitely many polynomials $f_1(x)$, such that $f_{k+1}(x)$ is the only term in the sequence $\{f_i(x)\}_{i=1}^{\infty}$ that is reducible. As a first corollary, we deduce that there exist infinitely many polynomial Cunningham chains of length k of both kinds, and as a second corollary, we have that, unlike the situation in the integers, there exist infinitely many polynomial Cunningham chains of infinite length of both kinds.

1. INTRODUCTION

We begin by giving the definitions of standard Cunningham chains [R].

Definition 1.1. Let $\epsilon \in \{-1, 1\}$. A sequence of prime numbers $p_1, p_2, p_3, \ldots$, such that $p_i = 2p_{i-1} + \epsilon$ for all i, is called a *Cunningham chain* of the first or second kind, depending on whether $\epsilon = 1$ or -1 respectively. If k is the smallest positive integer such that $2p_k + \epsilon$ is composite, then we say the chain has length k.

We define polynomial Cunningham chains in a similar manner.

Definition 1.2. A sequence of polynomials $f_1(x), f_2(x), \ldots$, such that $f_i(x) \in \mathbb{Z}[x]$, $f_1(x)$ has positive leading coefficient, $f_i(x)$ is irreducible over $\mathbb{Q}$, and $f_i(x) = xf_{i-1}(x) + \epsilon$ for all i, is called a *polynomial Cunningham chain* of the first or second kind, depending on whether $\epsilon = 1$ or -1 respectively. If k is the least positive integer such that $f_{k+1}(x)$ is reducible over $\mathbb{Q}$, then we say the chain has length k.

Remark 1.3. Note that if the restriction in Definition 1.2 that $f_1(x)$ have positive leading coefficient is dropped, then any chain of the first or second kind, with first term $f_1(x)$, produces a chain of the other kind with the exact same irreducibility properties by simply allowing the first term to be $-f_1(x)$.

Although, using Fermat's little theorem, it is straightforward to show that Cunningham chains are necessarily finite, it is conjectured that for any positive integer k, there exist infinitely many Cunningham chains of length k. This conjecture follows from either Dickson's conjecture [D, R] or Schinzel's hypothesis H [R, SS], but it is unlikely to be proven unconditionally in the near future. Currently, the longest known Cunningham chain is of length 17. In this article, we establish the analogous conjecture for polynomial Cunningham chains, and we also show that polynomial Cunningham chains can be infinite in length. More precisely, we prove the following.

Theorem 1.4. *For $\epsilon \in \{-1, 1\}$, and a given polynomial $f_1(x)$, we define a sequence $\{f_i(x)\}_{i=1}^{\infty}$ of polynomials by $f_i(x) = x f_{i-1}(x) + \epsilon$ for $i \geq 2$.*

(1) Let $\epsilon = 1$. Let $m \geq 2$ and $k \geq 1$ be integers. Define

$$f_1(x) := m^2 x^{k+3} + m x^{k+2} + m x^{k+1} + \cdots + m x + 1.$$

Then $f_i(x)$ is reducible over $\mathbb{Q}$ if and only if $i = k + 1$.

(2) Let $\epsilon = -1$. Let k and m be positive integers with $m^2 > k+1$. Define

$$f_1(x) := m^2 x - (m^2 - k).$$

Then $f_i(x)$ is reducible over $\mathbb{Q}$ if and only if $i = k + 1$.

Corollary 1.5 is immediate from Theorem 1.4, and Corollary 1.6 follows from Theorem 1.4 by considering sequences $\{g_i(x)\}_{i=1}^{\infty}$, with $g_1(x) := f_{k+2}(x)$, and $g_i(x) = x g_{i-1}(x) + \epsilon$ for $i \geq 2$.

Corollary 1.5. *For every positive integer k, there exist infinitely many polynomial Cunningham chains (of both kinds) of length k.*

Corollary 1.6. *There exist infinitely many polynomial Cunningham chains (of both kinds) of infinite length.*

2. Preliminaries

We begin this section with some more definitions and notation, and we let $f(x) \in \mathbb{Z}[x]$ throughout this section.

Definition 2.1. The *reciprocal* of $f(x)$ is defined to be the polynomial $\widetilde{f}(x) := x^{\deg f} f\left(\dfrac{1}{x}\right)$. We say that $f(x)$ is *reciprocal* if $f(x) = \pm \widetilde{f}(x)$, and *nonreciprocal* otherwise.

Definition 2.2. Suppose $f(0) \neq 0$, and that $f(x)$ factors over $\mathbb{Q}$ into irreducibles as $g_1(x) g_2(x) \cdots g_k(x)$, where $g_i(x)$ is reciprocal with positive leading coefficient, exactly when $0 \leq i \leq j$. Then $g_1(x) g_2(x) \cdots g_j(x)$ is called

the *reciprocal part of f* and $g_{j+1}(x) \cdots g_k(x)$ is called the *nonreciprocal part of f*.

If $f(0) \neq 0$, then it is clear from Definition 2.1 that $\deg f = \deg \widetilde{f}$ and $\widetilde{\widetilde{f}}(x) = f(x)$. Then, in this situation, $f(x) = g(x)h(x)$ if and only if $\widetilde{f}(x) = \widetilde{g}(x)\widetilde{h}(x)$. Therefore, we have the following:

Proposition 2.3. *Suppose that $f(0) \neq 0$. Then $f(x)$ is irreducible over $\mathbb{Q}$ if and only if $\widetilde{f}(x)$ is irreducible over $\mathbb{Q}$.*

The following theorem due to Fried and Schinzel [FS], which we state without proof, is needed to establish our results. We let $\exp_2(\alpha)$ denote $\exp(\exp(\alpha))$ for any expression α.

Theorem 2.4. *Let a, b, c, d be any nonzero integers, $m > n > p$ any positive integers, and assume that $q(x) = ax^m + bx^n + cx^p + d$ is not the product of two binomials. Then the nonreciprocal part of $q(x)$ is reducible if and only if one of the following cases holds:*

(1) $q(x)$ can be divided into two parts which have a nonreciprocal common factor

(2) $q(x)$ can be represented in one of the three forms in $(*)$ below:

$$(*) \begin{cases} \xi(U^3 + V^3 + W^3 - 3UVW) \\ = \xi(U + V + W)(U^2 + V^2 + W^2 - UV - UW - VW), \\ \\ \xi(U^2 - 4TUVW - T^2V^4 - 4T^2W^4) \\ = \xi(U - TV^2 - 2TVW - 2TW^2)(U + TV^2 - 2TVW + 2TW^2), \\ \\ \xi(U^2 + 2UV + V^2 - W^2) = \xi(U + V + W)(U + V - W), \end{cases}$$

where $T, U, V, W \in \mathbb{Q}[x]$ are monomials, $\xi \in \mathbb{Q}$, and the factors appearing on the right hand side of each equation in $(*)$ are not reciprocal

(3) $m = vm_1$, $n = vn_1$, $p = vp_1$, where $v > 1$,

$$m_1 < \exp_2(3 \cdot 2^{a^2+b^2+c^2+d^2+2} \log(a^2 + b^2 + c^2 + d^2)),$$

and the non-reciprocal part of $ax^{m_1} + bx^{n_1} + cx^{p_1} + d$ is reducible.

3. Proof of Theorem 1.4

Proof of Theorem 1.4. For part *(1)*, we have by induction that

$$f_n(x) = m^2 x^{n+k+2} + mx^{n+k+1} + mx^{n+k} + \cdots + mx^n + x^{n-1} + x^{n-2} + \cdots + x + 1,$$

for all $n \geq 1$. Since

$$f_{k+1}(x) = \left(mx^{k+1} + x^k + \cdots + x + 1 \right) \left(mx^{k+2} + 1 \right),$$

we see that $f_n(x)$ is reducible when $n = k + 1$. To show that $f_n(x)$ is irreducible over $\mathbb{Q}$ for all $n \neq k + 1$, we show that

$$\widetilde{f_n}(x) = x^{n+k+2} + x^{n+k+1} + \cdots + x^{k+3} + mx^{k+2} + \cdots + mx + m^2$$

is irreducible over $\mathbb{Q}$ for all $n \neq k+1$, which is equivalent by Proposition 2.3. We first claim that all zeros of $\widetilde{f_n}(x)$ are in $|z| > 1$. Consider the polynomial

$$F_n(x) := (x - 1)\widetilde{f_n}(x) = x^{n+k+3} + (m - 1)x^{k+3} + (m^2 - m)x - m^2,$$

and let α be a zero of $F_n(x)$. If $|\alpha| < 1$, then

$$
\begin{aligned}
m^2 &= \left| \alpha^{n+k+3} + (m - 1)\alpha^{k+3} + (m^2 - m)\alpha \right| \\
&\leq |\alpha|^{n+k+3} + (m - 1)|\alpha|^{k+3} + (m^2 - m)|\alpha| \\
&< m^2,
\end{aligned}
$$

which is impossible. Hence, $|\alpha| \geq 1$. If $|\alpha| = 1$, then $\alpha = e^{i\theta} = \cos(\theta) + i\sin(\theta)$, for some $\theta \in [0, 2\pi)$. Thus,

$$\cos\left((n + k + 3)\theta\right) + (m - 1)\cos\left((k + 3)\theta\right) + (m^2 - m)\cos(\theta) = m^2,$$

which implies that $\theta = 0$, and so $\alpha = 1$. This establishes the claim that all zeros of $\widetilde{f_n}(x)$ are in $|z| > 1$. It follows that the nonreciprocal part of $F_n(x)$ is $\widetilde{f_n}(x)$.

We now use Theorem 2.4 with $q(x) := F_n(x)$ to show that $\widetilde{f_n}(x)$ is irreducible when $n \neq k + 1$. We see easily that

$$
\begin{aligned}
F_n(x) &= x^{n+k+3} + (m - 1)x^{k+3} + (m^2 - m)x - m^2 \\
&= (x^{\ell_1} + r_1)(x^{\ell_2} + r_2) \\
&= x^{\ell_1+\ell_2} + r_2 x^{\ell_1} + r_1 x^{\ell_2} + r_1 r_2
\end{aligned}
$$

is impossible by comparing coefficients. Thus, $F_n(x)$ is not the product of two binomials.

Next, we show that $F_n(x)$ cannot be any of the forms in $(*)$ in Theorem 2.4. First, assume that

$$F_n(x) = \xi(U^3 + V^3 + W^3 - 3UVW).$$

Then $-3\xi UVW = (m^2 - m)x$, and hence two of the three terms U^3, V^3, W^3 are constant, which is a contradiction.

Suppose next that

$$F_n(x) = \xi(U^2 - 4TUVW - T^2V^4 - 4T^2W^4).$$

If $\xi > 0$, then $-\xi T^2 V^4$ and $-4\xi T^2 W^4$ are negative terms, which is impossible. Thus, $\xi < 0$, and so $\xi U^2 = -m^2$. The parity of the exponents implies that $-4\xi TUVW = (m^2 - m)x$. Therefore, exactly two of T, V and W are constants. Since we have only the two possibilities

(3.1) $\qquad -\xi T^2 V^4 = x^{n+k+3} \quad$ and $\quad -4\xi T^2 W^4 = (m - 1)x^{k+3}, \quad$ or

(3.2) $-\xi T^2 V^4 = (m-1)x^{k+3}$ and $-4\xi T^2 W^4 = x^{n+k+3}$,

it follows that V and W must be constants. Then, since $-4\xi TUVW = (m^2 - m)x$, we have that T is divisible by x, but not x^2. However, by comparing exponents, we see then that both possibilities, (3.1) and (3.2), are impossible since $n + k + 3 \geq 5$.

Now suppose that

$$F_n(x) = \xi(U^2 + 2UV + V^2 - W^2).$$

If $\xi < 0$, then the terms ξU^2 and ξV^2 are both negative, which is impossible. Thus, $\xi > 0$, and so $-\xi W^2 = -m^2$. Then both U and V must be divisible by x, which implies that U^2, UV and V^2 are divisible by x^2. But this contradicts the fact that $F_n(x)$ contains the term $(m^2 - m)x$.

Also, the fact that $F_n(x)$ contains the linear term $(m^2 - m)x$ implies that case *(3)* does not apply in Theorem 2.4.

Next we consider if, and when, $F_n(x)$ can be divided into two parts which have a common nonreciprocal factor. There are three cases to check: $(g_1, g_2) =$

(i) $\left(x^{n+k+3} + (m-1)x^{k+3}, \quad (m^2 - m)x - m^2\right)$
(ii) $\left(x^{n+k+3} + (m^2 - m)x, \quad (m-1)x^{k+3} - m^2\right)$
(iii) $\left(x^{n+k+3} - m^2, \quad (m-1)x^{k+3} + (m^2 - m)x\right).$

In case (i), it is easy to see that g_1 and g_2 have no common nonreciprocal factor since $m/(m-1)$ is not a zero of g_1.

In case (ii), g_1/x is irreducible over $\mathbb{Q}$ by Eisenstein's criterion using any prime divisor of m. Thus, by considering degrees, we can rule out every possibility except $n = 1$. But, when $n = 1$, we see that $g_2/(m-1) \neq \pm g_1/x$, and hence g_1 and g_2 have no common nonreciprocal factor in this case.

For case (iii), let h be a common factor of g_1 and g_2. Then h divides

$$x^n \frac{g_2}{m-1} - g_1 = m\left(x^{n+1} + m\right),$$

so that h divides

$$x^{n+1} + m - \frac{g_2}{(m-1)x} = \begin{cases} -x^{n+1}\left(x^{k-n+1} - 1\right) & \text{if } n < k+1 \\ x^{k+2}\left(x^{n-k-1} - 1\right) & \text{if } n > k+1 \end{cases}$$

In either case, we see that h is reciprocal, which implies that $\widetilde{f_n}(x)$ is irreducible for all $n \neq k+1$. This completes the proof in the case of chains of the first kind.

To establish part *(2)* of the theorem, we have by induction that

$$f_n(x) = m^2 x^n - (m^2 - k)x^{n-1} - x^{n-1} - \cdots + x - 1,$$

for all $n \geq 1$. Since $f_{k+1}(1) = 0$, we see that $f_n(x)$ is reducible when $n = k+1$. To show that $f_n(x)$ is irreducible over $\mathbb{Q}$ for all $n \neq k+1$, it is enough, by Proposition 2.3, to show that

$$-\widetilde{f_n}(x) = x^n + x^{n-1} + \cdots + x^2 + (m^2 - k)x - m^2$$

is irreducible over $\mathbb{Q}$ for all $n \neq k+1$. Consider the polynomial

$$F_n(x) := -(x-1)\widetilde{f_n}(x) = x^{n+1} + (m^2 - k - 1)x^2 - (2m^2 - k)x + m^2.$$

We claim that $-\widetilde{f_n}(x)$ is the nonreciprocal part of $F_n(x)$ when $n \neq k+1$. Suppose, by way of contradiction, that α and $1/\alpha$ are both zeros of $F_n(x)$, with $\alpha \neq 1$. Then

$$(3.3) \qquad -\alpha^{n+1} = (m^2 - k - 1)\alpha^2 - (2m^2 - k)\alpha + m^2 \qquad \text{and}$$

$$(3.4) \qquad -\frac{1}{\alpha^{n+1}} = \frac{m^2 - k - 1}{\alpha^2} - \frac{2m^2 - k}{\alpha} + m^2.$$

Substituting the expression for $-\alpha^{n+1}$ from (3.3) into (3.4), rearranging and factoring, gives $(\alpha - 1)^2 g(\alpha) = 0$, where

$$g(x) = \left(m^4 - m^2 k - m^2\right)x^2 - \left(2m^4 - 2m^2 k + k^2 + k\right)x + m^4 - m^2 k - m^2.$$

Note that α and $1/\alpha$ are distinct positive real zeros of $g(x)$ since $m^2 > k+1$. However, by Descartes' rule of signs, $F_n(x)$ has two positive real zeros counting multiplicities, and since $-\widetilde{f_n}(1) = 0$ only when $n = k+1$, it follows that $F_n(x)$ has exactly one positive real zero $\beta \neq 1$ when $n \neq k+1$. This contradiction establishes the claim.

We now use Theorem 2.4 with $q(x) := F_n(x)$ to show that $\widetilde{f_n}(x)$ is irreducible when $n \neq k+1$. Since, as in the case of chains of the first kind, it is straightforward to show that $F_n(x)$ is not the product of two binomials, and that $F_n(x)$ cannot be any of the forms in $(*)$ in Theorem 2.4, we omit the details. Also, the fact that $F_n(x)$ contains a linear term implies that case (3) does not apply in Theorem 2.4.

Next we consider if, and when, $F_n(x)$ can be divided into two parts which have a common nonreciprocal factor. There are three cases to check: $(g_1, g_2) =$

  (i) $\left(x^{n+1} + (m^2 - k - 1)x^2, \quad -(2m^2 - k)x + m^2\right)$
  (ii) $\left(x^{n+1} - (2m^2 - k)x, \quad (m^2 - k - 1)x^2 + m^2\right)$
  (iii) $\left(x^{n+1} + m^2, \quad (m^2 - k - 1)x^2 - (2m^2 - k)x\right).$

It is easy to see in each of these cases, by examining the zeros of g_2, that g_1 and g_2 have no common nonreciprocal factor. Thus, $f_n(x)$ is irreducible if and only if $n \neq k+1$, which completes the proof of the theorem.

$\square$

4. Concluding Remarks

For each $\epsilon \in \{-1, 1\}$, Theorem 3 in [S], rather than Theorem 2.4, can be used to establish the existence of infinitely many polynomials $f_1(x)$, such that there is exactly one reducible polynomial in the sequence $\{f_i(x)\}_{i=1}^{\infty}$, where $f_i(x) = xf_{i-1}(x) + \epsilon$ for $i \geq 2$. However, the drawback is that the polynomials $f_1(x)$ have no set form using this approach, as do the polynomials $f_1(x)$ given in Theorem 1.4, and so they cannot be given explicitly. Along these lines we make the following conjecture.

Conjecture 4.1. *Let $k \geq 1$ be an integer. Let $t = 2\lceil \frac{k+1}{2}\rceil + 1$, and let $m = 2\left(\frac{2^t+1}{3}\right)$. Then*

$$x^j + x^{j-1} + \cdots + x + m,$$

where $j \geq t - k$, is reducible over $\mathbb{Q}$ if and only if $j = t$.

Corollary 1.6 can also be proven easily without the use of Theorem 2.4. In the case of $\epsilon = 1$, let p be a prime, and define $f_1(x) := px + 1$. In the case of $\epsilon = -1$, let c be any positive integer, define $f_1(x) := x - c$, and use the following result due to Alfred Brauer [B].

Theorem 4.2. *Let $f(x) = x^n - a_{n-1}x^{n-1} - a_{n-2}x^{n-2} - \cdots - a_1 x - a_0$. If $a_{n-1} \geq \cdots \geq a_0 > 0$, then $f(x)$ is irreducible over $\mathbb{Q}$.*

References

[B]   A. Brauer, *On algebraic equations with all but one root in the interior of the unit circle*, Math. Nachr., 4 (1951), 250–257.

[D]   L. E. Dickson, *A new extension of Dirichlet's theorem on prime numbers*, Messenger of Mathematics, 33 (1904), 155–161.

[FS] M. Fried and A. Schinzel, *Reducibility of quadrinomials*, Acta Arith., 21 (1972), 153–172.

[R]   P. Ribenboim, *The new book of prime number records*, 3rd ed., Springer-Verlag, New York, 1996.

[S]   A. Schinzel, *On reducible trinomials. III.*, Period. Math. Hungar. 43 (2001), no. 1-2, 43-69.

[SS] A. Schinzel and W. W. Sierpiński, *Sur certaines hypotheses concernment les nombres premiers*, Acta. Arith., 4 (1958), 185–208. Erratum 5 (1958).

DEPARTMENT OF MATHEMATICS, SHIPPENSBURG UNIVERSITY, PENNSYLVANIA, USA
E-mail address, Lenny Jones: `lkjone@ship.edu`